UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/675,652	09/30/2003	Jeyhan Karaoguz	15046US01	5798

23446 7590 09/04/2007

MCANDREWS HELD & MALLOY, LTD
500 WEST MADISON STREET
SUITE 3400
CHICAGO, IL 60661

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

mn

Office Action Summary	Application No.	Applicant(s)	
	10/675,652	KARAOGUZ ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 6/19/07.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-28 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-28 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-28 have been examined.

Response to Arguments

2. Applicant's arguments have been carefully considered.

3. Applicant argues, as it appears, that the claim 11 overcame the art of record based on applicant's arguments towards claim 1 and 18. The argument was not found persuasive. Claim 11 recites only a subset of the limitations in claim 1 and 18. For example, claim 11 does not comprise "attempting to identify acquired security data associated with the media peripheral, and if said security data is not found:", "exchanging information associated with the home" etc.

4. Applicant's arguments with respect to claims 1-10 and 18-28 are considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-10 and 18-28 are rejected under 35 U.S.C. 112, second paragraph, as failing to set forth the subject matter which applicant(s) regard as their invention.

6. Claims recite limitation "attempting to identify previously acquired security data, followed by "is said security data is not found". It is not clear how the security data is "previously acquired" if it is not found.

7. Furthermore, it is not clear whether "previously acquired security data" is to be treated as equivalent term to "said security data". For example, see claim 6 and 7. Claim 6 recite "if previously acquired security data" that suggests that may be but in light of claim 1, the limitations of claim 6 suggests that it should be "if the previously acquired security data".
8. Similar structures are observed in claims 18 and 23-24.
9. The term "attempting" in claims 1 and 18 is not understood. It is not clear whether the steps are or are not performed (identification of previously acquired security data). For purpose of the further examination the term is treated as "searching".
10. Claims 2-5, 8-10, 18-22 and 25-28 are rejected by virtue of their dependence. Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 11-17 remain rejected under 35 U.S.C. 103(a) as being unpatentable over Mikkonen (USPN 6822971) in view of Answell (USPN 6367019).

As per claims 2-17 and 19-28, Mikkonen (USPN 6822971) discloses a method for establishing secure access (a tunnel col. 8 lines 1-12) to a media peripheral

(PCMCIA card, e.g. object 62 (with a storage element 56)) via a node (e.g. agent 34 or 130) in a communication network (e.g. a network including a correspondent node/entity 22 Fig. 1, 154 Fig. 3, 154 Fig. 4 etc.), the method comprising: detecting when the media peripheral is communicatively coupled to the node (col. 7 lines 40-44); acquiring data associated with the media peripheral, registering media peripheral (for subsequent operation) and utilizing the acquired data to facilitate secure communication between the media peripheral and the communication network (col. 7 line 44- col. 8 line 12). Mikonnen discloses reading the data from the media peripheral (col. 6 lines 28-43 col. 7 lines 1-17 and col. 7). The examiner considers the node to be a media exchange server and points to Fig. 2 that discloses the data comprising at least one user identifier.

12. Mikkonen is silent regarding the data (e.g. data distributed to the media exchange server, as discussed above) to be security data (such as a digital certificate) and does not disclose authentication the security data.

Ansell discloses a media peripheral providing security data (such as digital certificate) that is authenticated (Ansell, col. 9 line 58- col. 10 line 55).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include the security data (such as digital certificate) that could be authenticated as disclosed by Ansell. One of ordinary skill in the art would have been motivated to perform such a modification in order to provide secure communication with an authenticated party (Ansell, col. 2 lines 46-67).

13. Claims 1-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Anderson (Fredrik Andersson and Magnus Karlsson, "Secure Jini Services in Ad Hoc Networks", 2000).

As per claims 1-2, 4-5, 7, 9-12, 14-17, 18-24 and 26-28, Anderson discloses a home network (Fig. 8.1), wherein a client offering a service (server, pg. 37) registers an offered service at the Lookup Server (pg. 41) by uploading a part of the service (proxy) to the Lookup Server. (7.2.1) "Services can be any kind of small indicators, such as lamp-switches, to really complex devices, such as printers or copy-machines." (3.5.1) The service (proxy) bundled in .jar-file which also includes a certificate of the service. (8.2.3, certificate) "When a user receives the .jar-file, it can easily check who has signed the code". (8.2.3) "The check of a validity of a certificate can be done by calculating a unique checksum over the certificate" that is transferred to the service user, which checks validity of the certificate (8.2.4). "When the client receives the implementation from the server, it is delivered as a signed compressed jar-file. The jar-file beside the implementation classes also contains a certificate and a signature file. The client now retrieves the certificate and by doing that, he makes certain that the code was not altered or the sender was faked". (8.3.2 pg. 52)

Anderson suggests that the client keeps previously read said security data (certificate) that originated from the media peripheral. Caching previously stored security data is old and well known in the art of computing (e.g. a cookie) and as a result it would have been obvious to one of ordinary skill in the art at the time of

applicant's invention to attempt to identify previously acquired security data associated with the media peripheral given the benefit of potential time and bandwidth saving since no data transfer would be required.

14. Client not finding the security data resulting in downloading and validating (authenticating) a certificate of a service providing by a previously acquired security data associated with a media peripheral from a Lookup Server (a media exchange server) reads on "if the media peripheral is not found, exchanging information associated with the home and acquiring security data associated with the media peripheral".

15. Client's certificate validating and communicating with the media peripheral for the offered service reads on "utilizing said acquired security data associated with the media peripheral to facilitate secure communication between the media peripheral and the communication network".

16. Client's certificate validating and communicating with the media peripheral to receive the offered service reads on "validating said acquired security data prior to communicating over the communication network".

17. Anderson discloses the certificate includes at least one identifier associated with the home (e.g. manifest.mf-entry 8.2.3).

18. As per claims 3 and 13, since the security data is originated at the media peripheral before distribution (and authentication) of the data over network this reads on "reading the security data from the media peripheral".

19. As per claims 6 and 26, Client downloading and validating a certificate of a service providing media peripheral such as a printer from a Lookup Server reads on "attempting to identify previously acquired security data associated with the media peripheral and if the media peripheral is found, acquiring at least one identifier associated with the home". (Note that the certificate includes at least one identifier associated with the home (e.g. manifest.mf-entry 8.2.3), for example).
20. Client's (processor's) certificate validating and communicating with the media peripheral for the offered service reads on "validating said acquired security data prior to communicating over the communication network".".
21. As per claims 8, 16 and 25 the media peripheral is accessed after it is registered/initialized.
22. As per claims 9 and 26, Anderson discloses at least one user identifier (person's ral fingerprint, pg. 45-46).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)

8/30/07

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER